

BC - what to find

🔥 Tier 1 — Highest Payoff, Lowest Friction (Start Here)

1. Municipal Network Diagrams & Firewall Approvals

Why #1:

- These *must* exist if anything touched a network.
- DeepSeek confirms that comparable Canadian municipalities routinely generate network architecture and segmentation diagrams for election systems.
- They cut through narrative instantly.

What you get:

- Listener placement (LAN / DMZ / routable segment)
- Cellular transmission pathways and segmentation
- Internet ingress/egress paths
- Whether “firewalled” meant *isolated* or merely *filtered*

Effort: Low

Payoff: Extremely high

If this contradicts the doc, the doc collapses.

2. Election Operations Manuals / SOPs

Why #2:

- This is where *deployment truth* lives.
- DeepSeek identifies SOPs and training manuals as standard operational artefacts generated to support results transmission systems.
- Staff don’t run on marketing language.

What you get:

- Whether RTM / modems were trained, optional, discouraged, or prohibited
- Step-by-step instructions for results transmission and failure handling
- Whether “real-time” was operational or aspirational
- Incident-response guidance for transmission or equipment failure

Effort: Low

Payoff: Very high

3. Asset & Inventory Records (Modems, Laptops, SIMs)

Why #3:

- Physical assets don’t lie.
- DeepSeek confirms that asset inventories and telecom agreements are routinely generated for election technology deployments.
- “Optional” equipment leaves purchase trails.

What you get:

- Whether cellular modems were actually purchased
- Whether SIMs or private APNs were provisioned
- How many RTM-capable laptops existed
- Whether hardware scale matches an “offline-only” narrative

Effort: Low–medium

Payoff: Very high

This quietly answers the offline question.

🟡 Tier 2 — Medium Effort, Strong Contextual Proof

4. Procurement Evaluation & Security Scoring Records

Why #4:

- Shows what the City *cared about*, not what vendors claimed.
- DeepSeek identifies procurement justifications, IT approvals, and risk assessments as standard artefacts in comparable municipalities.

What you get:

- Whether “not connected to the Internet” was treated as a hard requirement
- Whether modems / RTM were flagged as risks or mitigations
- IT security sign-offs or third-party review notes
- Any dissenting opinions or documented risk trade-offs

Effort: Medium

Payoff: High (intent + governance)

5. Public Statements / Media Briefings

Why #5:

- Officials speak loosely here.
- Drift = signal.

What you get:

- Plain-language descriptions of connectivity
- Explanations that simplify or contradict formal documents
- Statements that exceed the precision of FOI materials

Effort: Low

Payoff: Medium–high

Great for contradiction mapping.

 Tier 3 — Harder, Decisive (But Gated)

6. Vendor Training & Support Materials

Why #6:

- Reveals real assumptions engineers make.
- DeepSeek notes that training decks and support materials often surface operational realities not present in contracts.

What you get:

- Expected internet availability
- VPN usage norms
- Field troubleshooting logic
- Practical fallback workflows under failure conditions

Effort: Medium–high

Payoff: High

But harder to obtain cleanly.

7. Logs (Firewall / VPN / EMS / Listener)

Why #7:

- This is the truth layer.
- Logs only matter *after* all prior artefacts exist.

What you get:

- Actual network activity
- Remote access evidence
- Transmission timelines
- Ground-truth operational behavior

Effort: High

Payoff: Absolute

Requires escalation.

 Not Worth Chasing (Right Now)

- Source code
- Hypothetical exploits
- Other jurisdictions' scandals
- Social media speculation

These dilute your position.

 Optimal Path (if you’re surgical)

One FOI can hit the top 3 at once:

- Network diagrams & firewall approvals
- Election operations manuals / SOPs
- Asset inventories and telecom agreements for election hardware

That’s the **80/20 strike**.